SENTRY:

[Proposed Implementation](#h.3t6ej53shc4f)

[Users and Views](#h.qqbdpc53gw6w)

[View definitions](#h.xqcx81sui4pk)

[Specifying who has access to data](#h.xdk8e4w77y2p)

[Installation (condensed) To-do list:](#h.skl1rbpud4pw)

[Sentry add-on Installation](#h.8dl70flxfiz3)

[Impala installation:](#h.1fgpnbge7smy)

[Syncing the Unix users/groups into Hue with these commands:](#h.u8osp9jxtqf)

# Proposed Implementation

This document presents an implementation based on 4 views and an Admin, delineated as follows:

1. Read only.
2. Read-write (non-critical/ non-private data)
3. Read-write (all data, based on open schema)
4. An admin read-write level (all data, no-restrictions)
5. An Unix Admin level, which controls all other levels, and is not restricted at all.

The 5 level permissions plan is shown from least amount of permission to greatest. The “View” names can be changed to YourCompanyDomain schema if needed. The “Views” are created to help organize sections of viewable data by permission level.

Each area of data in the filesystem can be configured to allow groups, with different permission-levels, to have access. Which means that **each user should either be allowed to have consistent fixed level access across the board, or else views should be written specifically for each data zone, and the users system group should be constrained to using them in the UI**. Here we describe a simple way to organize these views, by data-location, and user level.

The HDFS ACL’s work hand-in hand with the Sentry system, as it only allows authorized services to access the filesystem data, and will then dissect which data to show, based on a Sentry role, or view, for that user.

This document concentrates on formations of Sentry roles for users based on their respective FreeIPA groups.

**Note:**  A user may belong to multiple groups.

**Note:** Sentry groups can be synced to ACL’s via the bash scripts located in the /Hue\_Home/lib directory.

**Note:** Here Hue groups are used in lieu of Unix defined groups. Changes to follow D.R. plan.

## Users and Views

|  |  |  |
| --- | --- | --- |
| **Security Levels :** | | |
| **Role** | **Unix Group / Users** | **View that is created** |
| Trainee | “none” | View\_basic: Database: TBD (view only, restricted)  All INSERT/DELETE COMMANDS DISABLED |
| Analyst 1 | “base\_users” | View\_lvl1: Database: “Final”  Tables: Based on schema view (advanced/restricted) |
| Analyst 2 | “developers” | View\_lvl2: Database : TBD  Tables: Based on schema view. (Advanced level) |
| All-access  (non-admin) | “power\_users” | View\_all : All databases, and tables are available for INSERT/DELETE |
| ADMIN | UNIX ADMINS | ALL INSERT/DELETE COMMANDS |

## View definitions

All views to be prepended with data specific suffic; eg; “Instances\_lvl1”, “Instances\_all”

|  |  |  |
| --- | --- | --- |
| **“Instances” view** | | |
| View | Roles | Definition **(EXAMPLE)** |
| Insta\_basic |  | SELECT:  col1, col2, col3, col8 |
| Insta\_lvl1 |  | SELECT:  col1, col2, col3, col4, col8-12 |
| Insta\_lvl2 |  | SELECT  col1, col2, col3, col4, col8  SELECT,INSERT,DELETE  col3, col5, col7-10 |
| Insta\_all |  | SELECT,INSERT,DELETE  col1, col2, col3, col4, col8 |
| ADMIN |  | NO RULE |

## Specifying who has access to data

|  |  |  |
| --- | --- | --- |
| **“SalesForce” view** | | |
| View | Roles | Definition **(EXAMPLE)** |
| Sales\_basic |  | SELECT:  col1, col2, col3, col8 |
| Sales\_lvl1 |  | SELECT:  col1, col2, col3, col4, col8-12 |
| Sales\_lvl2 |  | SELECT  col1, col2, col3, col4, col8  SELECT,INSERT,DELETE  col3, col5, col7-10 |
| Sales\_all |  | SELECT,INSERT,DELETE  ALL |
| ADMIN |  | NO RULE |

|  |  |  |
| --- | --- | --- |
| **“Leaderboard” view** | | |
| View | Roles | Definition **(EXAMPLE)** |
| View\_basic |  | SELECT:  col1, col2, col3, col8 |
| View\_lvl1 |  | SELECT:  col1, col2, col3, col4, col8-12 |
| View\_lvl2 |  | SELECT  col1, col2, col3, col4, col8  SELECT,INSERT,DELETE  col3, col5, col7-10 |
| View\_all |  | SELECT,INSERT,DELETE  ALL |
| ADMIN |  | NO RULE |

|  |  |  |
| --- | --- | --- |
| **“Metablueprint” view** | | |
| View | Roles | Definition **(EXAMPLE)** |
| View\_basic |  | SELECT:  col1, col2, col3, col8 |
| View\_lvl1 |  | SELECT:  col1, col2, col3, col4, col8-12 |
| View\_lvl2 |  | SELECT  col1, col2, col3, col4, col8  SELECT,INSERT,DELETE  col3, col5, col7-10 |
| View\_all |  | SELECT,INSERT,DELETE  ALL |
| ADMIN |  | NO RULE |

|  |  |  |
| --- | --- | --- |
| **Sample-1 “Sample Table”** | | |
| Role | Data | Definition |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Continued on next page….

SENTRY :

# Installation (condensed) To-do list:

## **Sentry** add-on Installation

**[Install and sync HDFS / Sentry](http://www.cloudera.com/documentation/enterprise/5-4-x/topics/sg_hdfs_sentry_sync.html)**

Change Hue DB to Postgresql from Sqlite3.

[Creating and loading Hue SQL](http://www.cloudera.com/documentation/enterprise/5-2-x/topics/cm_mc_hue_service.html)

Inspecting the default Hue database (sqlite):  
sqlite3 /usr/share/hue/desktop/desktop.dbHive/warehouse: ownership and 770

Hive server impersonation: off

## Impala installation:

[Impala web servers](http://www.cloudera.com/documentation/enterprise/latest/topics/cm_mc_impala_service.html?scroll=xd_583c10bfdbd326ba-5676e95c-13ed333c3d9--8000)

[Impala requirements](http://www.cloudera.com/documentation/cdh/5-1-x/Impala/Installing-and-Using-Impala/ciiu_prereqs.html?scroll=prereqs)

[Impala concepts and architecture](http://www.cloudera.com/documentation/cdh/5-1-x/Impala/Installing-and-Using-Impala/ciiu_concepts.html#intro_hive_unique_2)

[Impala Installation with CM](http://www.cloudera.com/documentation/enterprise/latest/topics/cm_ig_install_impala.html) (Hosts:parcels, add impala repo, [configuration](http://www.cloudera.com/documentation/enterprise/latest/topics/cm_mc_impala_service.html?scroll=xd_583c10bfdbd326ba-5676e95c-13ed333c3d9--8000))

## Syncing the Unix users/groups into Hue with these commands:

|  |
| --- |
| build/env/bin/hue useradmin\_sync\_with\_unix --min-uid=1000 |

## 